Discrete Mathematics & Mathematical Reasoning
Arithmetic Modulo m, Primes

Colin Stirling

Informatics

Division

Definition

If a and b are integers with $a \neq 0$, then a divides b, written $a|b$, if there exists an integer c such that $b = ac$.

b is a multiple of a and a is a factor of b

Division

Definition

If a and b are integers with $a \neq 0$, then a divides b, written $a|b$, if there exists an integer c such that $b = ac$.

b is a multiple of a and a is a factor of b

$3 \mid (-12)$ $3 \mid 0$ $3 \not| 7$ (where $\not|$ "not divides")

Division

Definition

If a and b are integers with $a \neq 0$, then a divides b, written $a|b$, if there exists an integer c such that $b = ac$.

b is a multiple of a and a is a factor of b

$3 \mid (-12)$ $3 \mid 0$ $3 \not| 7$ (where $\not|$ "not divides")

Theorem

1. *If $a|b$ and $a|c$, then $a|(b + c)$*
2. *If $a|b$, then $a|bc$*
3. *If $a|b$ and $b|c$, then $a|c$*

Division

Definition

If a and b are integers with $a \neq 0$, then a divides b, written $a|b$, if there exists an integer c such that $b = ac$.

b is a multiple of a and a is a factor of b

$3 \mid (-12)$ $3 \mid 0$ $3 \nmid 7$ (where $\nmid$ "not divides")

Theorem

1. *If $a|b$ and $a|c$, then $a|(b+c)$*
2. *If $a|b$, then $a|bc$*
3. *If $a|b$ and $b|c$, then $a|c$*

Proof.

We just prove the first; the others are similar. Assume $a|b$ and $a|c$. So, there exists integers d, e such that $b = da$ and $c = ea$. So $b + c = da + ea = (d + e)a$ and, therefore, $a|(b + c)$. □

Division algorithm (not really an algorithm!)

Theorem

If a is an integer and d a positive integer, then there are unique integers q and r, with $0 \leq r < d$, such that $a = dq + r$

Division algorithm (not really an algorithm!)

Theorem

If a is an integer and d a positive integer, then there are unique integers q and r, with $0 \leq r < d$, such that $a = dq + r$

q is quotient and r the remainder; $q = a \text{ div } d$ and $r = a \bmod d$

Division algorithm (not really an algorithm!)

Theorem

If a is an integer and d a positive integer, then there are unique integers q and r, with $0 \leq r < d$, such that $a = dq + r$

q is quotient and r the remainder; $q = a \text{ div } d$ and $r = a \bmod d$

$a = 102$ and $d = 12$ $\quad$ $q = 8$ and $r = 6$ $\quad$ $102 = 12 \cdot 8 + 6$

Division algorithm (not really an algorithm!)

Theorem

If a is an integer and d a positive integer, then there are unique integers q and r, with $0 \leq r < d$, such that $a = dq + r$

q is quotient and r the remainder; $q = a \text{ div } d$ and $r = a \bmod d$

$a = 102$ and $d = 12$ $q = 8$ and $r = 6$ $102 = 12 \cdot 8 + 6$

$a = -14$ and $d = 6$ $q = -3$ and $r = 4$ $-14 = 6 \cdot (-3) + 4$

Division algorithm (not really an algorithm!)

Theorem

If a is an integer and d a positive integer, then there are unique integers q and r, with $0 \leq r < d$, such that $a = dq + r$

q is quotient and r the remainder; $q = a \text{ div } d$ and $r = a \bmod d$

$a = 102$ and $d = 12$ $q = 8$ and $r = 6$ $102 = 12 \cdot 8 + 6$
$a = -14$ and $d = 6$ $q = -3$ and $r = 4$ $-14 = 6 \cdot (-3) + 4$

Proof.

Let q be the largest integer such that $dq \leq a$; then $r = a - dq$ and so, $a = dq + r$ for $0 \leq r < d$: if $r \geq d$ then $d(q+1) \leq a$ which contradicts that q is largest. So, there is at least one such q and r. Assume that there is more than one: $a = dq_1 + r_1$, $a = dq_2 + r_2$, and $(q_1, r_1) \neq (q_2, r_2)$. If $q_1 = q_2$ then $r_1 = a - dq_1 = a - dq_2 = r_2$. Assume $q_1 \neq q_2$; now we obtain a contradiction; as $dq_1 + r_1 = dq_2 + r_2$, $d = (r_1 - r_2)/(q_2 - q_1)$ which is impossible because $r_1 - r_2 < d$. □

Congruent modulo m relation

Definition

If a and b are integers and m is a positive integer, then a is congruent to b modulo m, written $a \equiv b \pmod{m}$, iff $m | (a - b)$

- $17 \equiv 5 \pmod{6}$ because 6 divides $17 - 5 = 12$

Congruent modulo m relation

Definition

If a and b are integers and m is a positive integer, then a is congruent to b modulo m, written $a \equiv b \pmod{m}$, iff $m | (a - b)$

- $17 \equiv 5 \pmod{6}$ because 6 divides $17 - 5 = 12$
- $-17 \not\equiv 5 \pmod{6}$ because $6 \not| (-22)$

Congruent modulo m relation

Definition

If a and b are integers and m is a positive integer, then a is congruent to b modulo m, written $a \equiv b \pmod{m}$, iff $m | (a - b)$

- $17 \equiv 5 \pmod{6}$ because 6 divides $17 - 5 = 12$
- $-17 \not\equiv 5 \pmod{6}$ because $6 \not| (-22)$
- $-17 \equiv 1 \pmod{6}$

Congruent modulo m relation

Definition

If a and b are integers and m is a positive integer, then a is congruent to b modulo m, written $a \equiv b \pmod{m}$, iff $m | (a - b)$

- $17 \equiv 5 \pmod{6}$ because 6 divides $17 - 5 = 12$
- $-17 \not\equiv 5 \pmod{6}$ because $6 \not| (-22)$
- $-17 \equiv 1 \pmod{6}$
- $24 \not\equiv 14 \pmod{6}$ because $6 \not| 10$

Congruence is an equivalence relation

Theorem

$a \equiv b \ (mod\ m)$ *iff* $a \ mod\ m = b \ mod\ m$

Congruence is an equivalence relation

Theorem

$a \equiv b \pmod{m}$ iff $a \bmod m = b \bmod m$

Proof.

Assume $a \equiv b \pmod{m}$; so $m|(a-b)$. If $a = q_1 m + r_1$ and $b = q_2 m + r_2$ where $0 \leq r_1 < m$ and $0 \leq r_2 < m$ it follows that $r_1 = r_2$ and so $a \bmod m = b \bmod m$. If $a \bmod m = b \bmod m$ then a and b have the same remainder so $a = q_1 m + r$ and $b = q_2 m + r$; therefore $a - b = (q_1 - q_2)m$, and so $m|(a-b)$. □

Congruence is an equivalence relation

Theorem

$a \equiv b \pmod{m}$ iff $a \bmod m = b \bmod m$

Proof.

Assume $a \equiv b \pmod{m}$; so $m|(a-b)$. If $a = q_1 m + r_1$ and $b = q_2 m + r_2$ where $0 \leq r_1 < m$ and $0 \leq r_2 < m$ it follows that $r_1 = r_2$ and so $a \bmod m = b \bmod m$. If $a \bmod m = b \bmod m$ then a and b have the same remainder so $a = q_1 m + r$ and $b = q_2 m + r$; therefore $a - b = (q_1 - q_2)m$, and so $m|(a-b)$. □

- $\equiv \pmod{m}$ is an equivalence relation on integers

A simple theorem of congruence

Theorem

$a \equiv b \pmod{m}$ iff there is an integer k such that $a = b + km$

A simple theorem of congruence

Theorem

$a \equiv b \pmod{m}$ iff there is an integer k such that $a = b + km$

Proof.

If $a \equiv b \pmod{m}$, then by the definition of congruence $m|(a-b)$. Hence, there is an integer k such that $a - b = km$ and equivalently $a = b + km$. If there is an integer k such that $a = b + km$, then $km = a - b$. Hence, $m|(a-b)$ and $a \equiv b \pmod{m}$. □

Congruences of sums, differences, and products

Theorem

If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a + c \equiv b + d \pmod{m}$ and $ac \equiv bd \pmod{m}$

Congruences of sums, differences, and products

Theorem

If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a + c \equiv b + d \pmod{m}$ and $ac \equiv bd \pmod{m}$

Proof.

Since $a \equiv b$ (mod m) and $c \equiv d \pmod{m}$, by the previous theorem, there are integers s and t with $b = a + sm$ and $d = c + tm$. Therefore, $b + d = (a + sm) + (c + tm) = (a + c) + m(s + t)$, and $bd = (a + sm)(c + tm) = ac + m(at + cs + stm)$. Hence, $a + c \equiv b + d \pmod{m}$ and $ac \equiv bd \pmod{m}$ □

Congruences of sums, differences, and products

Theorem

If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a + c \equiv b + d \pmod{m}$ and $ac \equiv bd \pmod{m}$

Proof.

Since $a \equiv b$ (mod m) and $c \equiv d \pmod{m}$, by the previous theorem, there are integers s and t with $b = a + sm$ and $d = c + tm$. Therefore,
$b + d = (a + sm) + (c + tm) = (a + c) + m(s + t)$, and
$bd = (a + sm)(c + tm) = ac + m(at + cs + stm)$. Hence,
$a + c \equiv b + d \pmod{m}$ and $ac \equiv bd \pmod{m}$ □

Corollary

- $(a + b) \text{ mod } m = ((a \text{ mod } m) + (b \text{ mod } m)) \text{ mod } m$
- $ab \text{ mod } m = ((a \text{ mod } m)(b \text{ mod } m)) \text{ mod } m$

Arithmetic modulo m

- $\mathbb{Z}_m = \{0, 1, \ldots, m-1\}$

Arithmetic modulo m

- $\mathbb{Z}_m = \{0, 1, \ldots, m-1\}$
- $+_m$ on $\mathbb{Z}_m$ is $a +_m b = (a+b) \bmod m$

Arithmetic modulo m

- $\mathbb{Z}_m = \{0, 1, \ldots, m-1\}$
- $+_m$ on $\mathbb{Z}_m$ is $a +_m b = (a+b) \bmod m$
- $\cdot_m$ on $\mathbb{Z}_m$ is define $a \cdot_m b = (a \cdot b) \bmod m$

Arithmetic modulo m

- $\mathbb{Z}_m = \{0, 1, \ldots, m - 1\}$
- $+_m$ on $\mathbb{Z}_m$ is $a +_m b = (a + b) \bmod m$
- $\cdot_m$ on $\mathbb{Z}_m$ is define $a \cdot_m b = (a \cdot b) \bmod m$
- Find $7 +_{11} 9$ and $-7 \cdot_{11} 9$

Arithmetic modulo m

- $\mathbb{Z}_m = \{0, 1, \ldots, m-1\}$
- $+_m$ on $\mathbb{Z}_m$ is $a +_m b = (a+b) \bmod m$
- $\cdot_m$ on $\mathbb{Z}_m$ is define $a \cdot_m b = (a \cdot b) \bmod m$
- Find $7 +_{11} 9$ and $-7 \cdot_{11} 9$
- $7 +_{11} 9 = (7+9) \bmod 11 \quad = \quad 16 \bmod 11 = 5$

Arithmetic modulo m

- $\mathbb{Z}_m = \{0, 1, \ldots, m-1\}$
- $+_m$ on $\mathbb{Z}_m$ is $a +_m b = (a+b) \bmod m$
- $\cdot_m$ on $\mathbb{Z}_m$ is define $a \cdot_m b = (a \cdot b) \bmod m$
- Find $7 +_{11} 9$ and $-7 \cdot_{11} 9$
- $7 +_{11} 9 = (7+9) \bmod 11 \quad = \quad 16 \bmod 11 = 5$
- $-7 \cdot_{11} 9 = (-7 \cdot 9) \bmod 11 \quad = \quad -63 \bmod 11 = 3$

Primes

Definition

A positive integer $p > 1$ is called prime iff the only positive factors of p are 1 and p. Otherwise it is called composite

Primes

Definition

A positive integer $p > 1$ is called prime iff the only positive factors of p are 1 and p. Otherwise it is called composite

Theorem (Fundamental Theorem of Arithmetic)

Every positive integer greater than 1 *can be written uniquely as a prime or as the product of its prime factors, written in order of nondecreasing size*

Primes

Definition

A positive integer $p > 1$ is called prime iff the only positive factors of p are 1 and p. Otherwise it is called composite

Theorem (Fundamental Theorem of Arithmetic)

Every positive integer greater than 1 *can be written uniquely as a prime or as the product of its prime factors, written in order of nondecreasing size*

$765 = 3 \cdot 3 \cdot 5 \cdot 17 = 3^2 \cdot 5 \cdot 17$

Proof of fundamental theorem

Theorem (Fundamental Theorem of Arithmetic)

Every positive integer greater than 1 *can be written uniquely as a prime or as the product of its prime factors, written in order of nondecreasing size*

Proof of fundamental theorem

Theorem (Fundamental Theorem of Arithmetic)

Every positive integer greater than 1 can be written uniquely as a prime or as the product of its prime factors, written in order of nondecreasing size

Showed by induction if $n > 1$ is an integer then n can be written as a product of primes

Proof of fundamental theorem

Theorem (Fundamental Theorem of Arithmetic)

Every positive integer greater than 1 can be written uniquely as a prime or as the product of its prime factors, written in order of nondecreasing size

Showed by induction if $n > 1$ is an integer then n can be written as a product of primes

Missing is uniqueness

Proof of fundamental theorem

Theorem (Fundamental Theorem of Arithmetic)

Every positive integer greater than 1 can be written uniquely as a prime or as the product of its prime factors, written in order of nondecreasing size

Showed by induction if $n > 1$ is an integer then n can be written as a product of primes

Missing is uniqueness

Lemma if p is prime and $p | a_1 a_2 \ldots a_n$ where each a_i is an integer, then $p | a_j$ for some $1 \leq j \leq n$

Proof of fundamental theorem

Theorem (Fundamental Theorem of Arithmetic)

Every positive integer greater than 1 can be written uniquely as a prime or as the product of its prime factors, written in order of nondecreasing size

Showed by induction if $n > 1$ is an integer then n can be written as a product of primes

Missing is uniqueness

Lemma if p is prime and $p|a_1 a_2 \ldots a_n$ where each a_i is an integer, then $p|a_j$ for some $1 \leq j \leq n$

By induction too

Proof of fundamental theorem

Theorem (Fundamental Theorem of Arithmetic)

Every positive integer greater than 1 can be written uniquely as a prime or as the product of its prime factors, written in order of nondecreasing size

Showed by induction if $n > 1$ is an integer then n can be written as a product of primes

Missing is uniqueness

Lemma if p is prime and $p|a_1a_2\ldots a_n$ where each a_i is an integer, then $p|a_j$ for some $1 \leq j \leq n$

By induction too

Now result follows

There are infinitely many primes

There are infinitely many primes

Lemma Every natural number greater than one is either prime or it has a prime divisor

There are infinitely many primes

Lemma Every natural number greater than one is either prime or it has a prime divisor

Follows from fundamental theorem

There are infinitely many primes

Lemma Every natural number greater than one is either prime or it has a prime divisor

Follows from fundamental theorem

Proof Suppose towards a contradiction that there are only finitely many primes $p_1, p_2, p_3, \ldots, p_k$. Consider the number $q = p_1 p_2 p_3 \ldots p_k + 1$, the product of all the primes plus one. By hypothesis q cannot be prime because it is strictly larger than all the primes. Thus, by the lemma, it has a prime divisor, p. Because $p_1, p_2, p_3, \ldots, p_k$ are all the primes, p must be equal to one of them, so p is a divisor of their product. So we have that p divides $p_1 p_2 p_3 \ldots p_k$, and p divides q, but that means p divides their difference, which is 1. Therefore $p \leq 1$. Contradiction. Therefore there are infinitely many primes.

The Sieve of Eratosthenes

How to find all primes between 2 and n?

The Sieve of Eratosthenes

How to find all primes between 2 and n?

A very inefficient method of determining if a number n is prime

Try every integer $i \leq \sqrt{n}$ and see if n is divisible by i

1. Write the numbers $2, \ldots, n$ into a list. Let $i := 2$

The Sieve of Eratosthenes

How to find all primes between 2 and n?

A very inefficient method of determining if a number n is prime

Try every integer $i \leq \sqrt{n}$ and see if n is divisible by i

1. Write the numbers $2, \ldots, n$ into a list. Let $i := 2$
2. Remove all strict multiples of i from the list

The Sieve of Eratosthenes

How to find all primes between 2 and n?

A very inefficient method of determining if a number n is prime

Try every integer $i \leq \sqrt{n}$ and see if n is divisible by i

1. Write the numbers $2, \ldots, n$ into a list. Let $i := 2$
2. Remove all strict multiples of i from the list
3. Let k be the smallest number present in the list s.t. $k > i$ and let $i := k$

The Sieve of Eratosthenes

How to find all primes between 2 and n?

A very inefficient method of determining if a number n is prime

Try every integer $i \leq \sqrt{n}$ and see if n is divisible by i

1. Write the numbers $2, \ldots, n$ into a list. Let $i := 2$
2. Remove all strict multiples of i from the list
3. Let k be the smallest number present in the list s.t. $k > i$ and let $i := k$
4. If $i > \sqrt{n}$ then stop else go to step 2

The Sieve of Eratosthenes

How to find all primes between 2 and n?

A very inefficient method of determining if a number n is prime

Try every integer $i \leq \sqrt{n}$ and see if n is divisible by i

1. Write the numbers $2, \ldots, n$ into a list. Let $i := 2$
2. Remove all strict multiples of i from the list
3. Let k be the smallest number present in the list s.t. $k > i$ and let $i := k$
4. If $i > \sqrt{n}$ then stop else go to step 2

Testing if a number is prime can be done efficiently in polynomial time [Agrawal-Kayal-Saxena 2002], i.e., polynomial in the number of bits used to describe the input number. Efficient randomized tests had been available previously.